Rate-Adaptive LDPC Reconciliation and Estimation in Quantum Key Distribution

Pisit Vanichchanunt[1], Tharathorn Phromsa-ard[2*], Patcharapong Treeviriyanupub[3], Paramin Sangwongngam[4], and Lunchakorn Wuttisittikulkij[2+]
[1]Department of Electrical and Computer Engineering, Faculty of Engineering,
King Mongkut's University of Technology North Bangkok (KMUTNB), Bangkok, Thailand
[2]Department of Electrical Engineering, Faculty of Engineering,
Chulalongkorn University (CU), Bangkok, Thailand.
[3]Department of Information Technology, Faculty of Science and Technology,
Phranakhon Rajabhat University (PNRU), Bangkok, Thailand
[4]National Electronics and Computer Technology Center (NECTEC),
National Science and Technology Development Agency (NSTDA), Pathum Thani, Thailand.
E-mail: [1]v_pisit@hotmail.com, [2*]tharathorn.phromsaard@gmail.com, [2]patcharapong@pnru.ac.th,
[3]paramin.sangwongngam@nectec.or.th, [2+]lunchakorn.w@chula.ac.th

Abstract: The key reconciliation method is proposed as one of the classical parts in Quantum Key Distribution (QKD) protocol. The proposed method aims to correct the transmission error after distribution of quantum key objects over a quantum channel. For error correction, Low-Density Parity-Check (LDPC) codes are adopted as the technique of source coding with side information or the Slepian-Wolf coding. In this work, rate adaptive LDPC reconciliation method based on puncturing and shortening technique with estimated Quantum Bit Error Rate (QBER) from only syndrome is studied. Its objective is to skip the step of quantum bit error rate (QBER) estimation by the traditional key sampling that increases the final secret key length in practice. This method also estimates reconciliation efficiency (f) in advance for determination of an optimal rate that reduces the interactive communication. From numerical results, it can be observed that the performance of our proposed schemes in terms of reconciliation efficiency and secret key throughput is superior to conventional Cascade, and fixed-rate compatible LDPC based protocols. Therefore, gain of these proposed schemes is suitable for the high-speed discrete-variable QKD applications.

1. Introduction

Quantum key distribution (QKD) [1] sheds the light on an important long-standing problem in the cryptography where the security of secret key exchanging is guaranteed by properties of quantum mechanics. Generally, the QKD protocol requires that the two parties (called *Alice* and *Bob*) are physically connected via a true secret channel called quantum channels and an error-free channel, typically classical public channel. In fact, the QKD protocol relies on the quantum mechanics and the quantum information processing by the experimental and theoretical studies of quantum optics. However, its appropriation is still obstructed by the low-key rates, which depend on both the detection of the quantum state at the optical hardware and the efficiency of purely classical information processing. Therefore, these post-processing algorithms have the ability to contribute for having higher-speed secret key generation with improve high efficient reconciliation protocol.

Previously, the most widely used key reconciliation process have applied the binary interactive procedure of error correction, such as the well-known BBBSS [2] and Cascade protocol [3] which are implemented in most of commercial products. However, they are based on a binary searching algorithm that requires several communication rounds between *Alice* and *Bob* through the public channel leading to low-speed key generation. To solve such a problem Winnow was proposed in [4]. It deploys a Hamming code, a simple class of error correction codes, to correct the errors in a block. Many applications for coding schemes have been proposed in [5−9]. These research works observed the performance evaluation of the reconciliation protocol in the terms of reconciliation efficiency that directly related to the percentage of disclosed information during the reconciliation step. Although, LDPC codes are attractive to offer the performance asymptotically close to capacity limit, the major drawback of LDPC codes is the complexity of the message-passing decoding algorithm [10−11] and requires large amounts of memory to store a huge sparse parity-check matrix during reconciliation process.

The aim of this work is to present an alternative promising key reconciliation protocol with efficient rate adaptive LDPC codes for the discrete-variable QKD system. The sifted keys of *Alice* and *Bob* are viewed as the input and the output over Galois field of two elements GF(2) of a binary symmetric channel (BSC). This method is based on puncturing and shortening technique with estimated quantum bit error rate and reconciliation efficiency. This proposed method is optimized in the crossover probability distribution obviously corresponds to the various error rates in QKD, and provides the improvement of the reconciliation efficiency by reducing the cost of communication resources.

The paper is organized as follows. The system model for Slepian-Wolf coding and its application reconciliation are discussed in Section 2. A proposed a rate-adaptive LDPC reconciliation with estimator based on Slepian-Wolf system method is presented in Section 3. The numerical results and discussions are described in Section 4, and finally the conclusions are provided in Section 5.

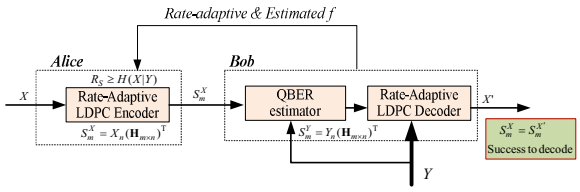

Figure 1. Rate-adaptive reconciliation using LDPC codes based on Slepian-Wolf coding..

2. Slepian-Wolf Coding and Its Application Reconciliation

The Slepian-Wolf coding problem for two correlated sources [12] is a problem of a near-lossless source coding with side information. There are two typical settings in the Slepian-Wolf coding problem when *Alice* and *Bob* have sifted keys *X* and *Y* respectively. First, *Alice* encodes *X* and sends compressed message *M* to *Bob*, then *Bob* recovers *X* using the source coding with side information sequence *Y* and *M*, which are both fed into the decoder for the result that will eventually become the recovered information *X'*. The objective of the key reconciliation process is to make the *Pr*[*X'*=*X*] close to one as much as possible. The amount of information leaked to *Eve* can be estimated from the number of bits in the side information source coding. Therefore, the efficiency of reconciliation and amount of leaked information |*M*| depends on the compression rate. Under the condition of Slepian-Wolf lower bound, $R_S \geq H(X \mid Y)$.

Let *C* be a linear block code which has a parity check matrix $\mathbf{H}$ of dimension $m \times n$. In the Slepian-Wolf scheme, the compression of main information X_n can be calculated by the syndrome *S* where $S_m^X = X_n(\mathbf{H}_{m\times n})^{\mathrm{T}}$. The compression rate of Slepian-Wolf code (R_S) and The channel coding rate (R_C) of linear code *C* are defined as $R_S = m/n$ and $R_C = (n-m)/n,$ respectively. The relation between the Slepian-Wolf compression rate and the channel coding rate can be represented as

$$R_S = 1 - R_C \tag{1}$$

In the reconciliation scheme, the channel coding rate R_C must be optimized as close to the Slepian-Wolf lower bound as possible. It was shown in the following equation

$$1 - R_C \geq H(X \mid Y) \tag{2}$$

In the case of QKD system, the quantum bit error rate (QBER) is equivalent to the crossover probability *e* of the BSC. Then, $H(X \mid Y)$ can be rewritten as

$$H(X \mid Y) = h(e) \triangleq -e\log_2(e) - (1-e)\log_2(1-e) \tag{3}$$

where $h(e)$ denotes the binary Shannon entropy.

3. Rate-Adaptive LDPC Reconciliation with Estimator based on Slepian-Wolf System

In this section, the proposed rate-adaptive LDPC reconciliation and estimation method is presented. It is designed based on LDPC codes [13] and the maximum-likelihood (ML) estimators [14] adapting to the Slepian-Wolf coding scheme. LDPC codes are binary linear block code specified by size $(n-k) \times n$ sparse parity check matrix $\mathbf{H}$ as (*n*, *k*) LDPC where *n, k* represent the codeblock length and the number of original information bits, respectively. The code rate can be calculated by $R_C = k/n.$ Puncturing and shortening technique are able to adapt the coding rate. When p punctured symbols of a codeword and s shorted symbols of the encoding process are removed. The coding rate is calculated as $C(n-p-s, n-s)$. The proportion of punctured and shortened symbols is $d = p + s$ and the ratio of modulate is $\delta = d/n.$

The proposed method can be constructed adaptively on its rate by using the Slepian-Wolf coding scheme as illustrated in Figure 1. The procedure of the proposed method is described by the following four steps:

Step 1) *Keys Generation*: *Alice* and *Bob* arrange their sifted keys X_n and Y_n, respectively, in a block of *n* bits . Both *Alice* X_n and *Bob* Y_n are correlated.

Step 2) *Syndrome encoding:* The sequences of X_n are fed into the LDPC-based Slepian-Wolf encoder for calculating her syndromes $S^X = X\mathbf{H}^{\mathrm{T}}$ with a high code rate $R_{\max}(p=d,\ s=0)$ and sends it to *Bob* over the public classical authenticated channel.

Step 3) *QBER and f estimation:* At *Bob*'s side, S_Y is also computed by $R_{\max}$. Then, the cross-over probability *e* of the correlated sources is calculated using the ML estimator from syndrome matching S_{diff} [14−15]. This can be defined as the binomial distribution of *q*(*e*) given by

$$\hat{q}(e) = \sum_{i=1}^{d_c} \binom{d_c}{i} e^i (1-\mathrm{e})^{d_c - 1} \tag{4}$$

where d_c is the average number of ones per row of parity check matrix $\mathbf{H}$ (check node degree). Then, the ML estimator for *e* with correspond to S_{diff} is the inverse function of (4) as

$$\hat{e}(S_{diff_m}) = f^{-1}(\hat{\mathrm{q}}(S_{diff_m})) = \frac{1-(1-2\hat{q}(S_{diff_m}))^{1/d_c}}{2} \tag{5}$$

where $\hat{q}(S_{Z_{n-k}}) = \frac{1}{n-k}\sum_{m=1}^{n-k} S_{diff_m}$ and $S_{diff} = S_X \oplus S_Y$

After this step, the knowledge of $\hat{e}$ can be applied to optimize the channel coding rate $R_C(\text{optimal})$, which are constrained with the fundamental key limit for estimation of reconciliation efficiency $f(n,\varepsilon,\hat{e})$ [16] as

$$f(n,\varepsilon,\hat{e}) = \eta_{LDPC}\left(1 + \frac{1}{\sqrt{n}}\frac{\sqrt{v(\hat{e})}}{h(\hat{e})}\Phi^{-1}(1-\varepsilon)\right) \tag{6}$$

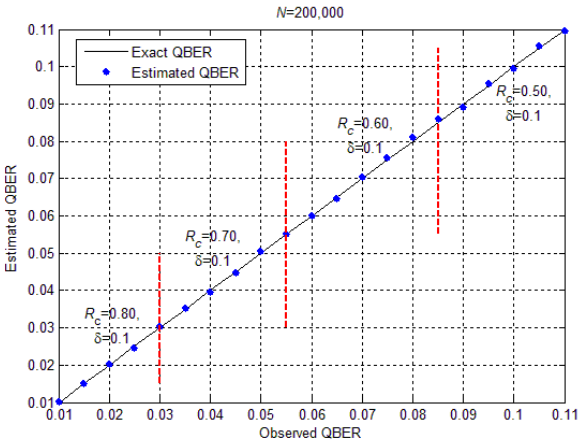

Figure 2. Estimated QBER as a function of observed QBER.

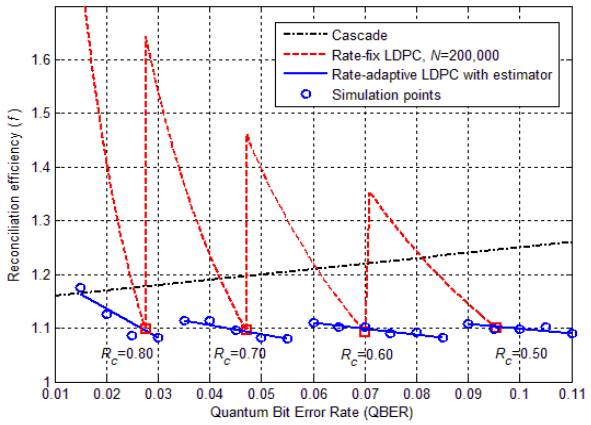

Figure 3. Reconciliation efficiency as a function of QBER.

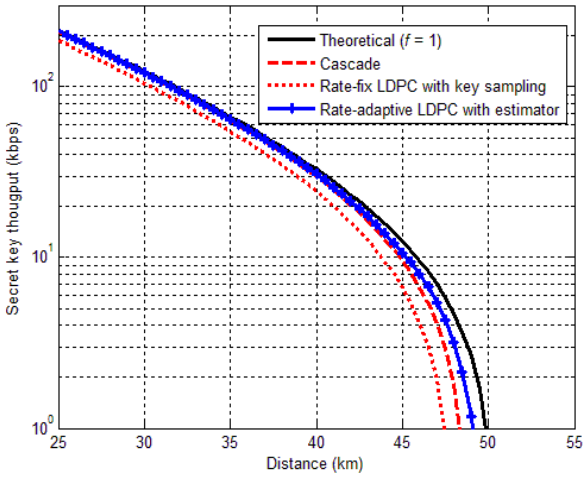

Figure 4. Secret key throughput as a function of distance

where $\hat{e}$ is estimated QBER, ε is Frame Error Rate (FER), $v(\hat{e}) = \hat{e}(1-\hat{e})(\log_2(\hat{e}/(1-\hat{e})))^2$ is conditional entropy variance, Φ is cumulative standard normal distribution and $\eta_{LDPC} \geq 1$ is reconciliation efficiency of LDPC codes. If $R_C(\text{optimal}) < R_{\max}$ they then return to Step 2 in order to change a number of p and s symbols as close to the Slepian-Wolf lower bound in

$$1 - R_C(\text{optimal}) = \frac{n-k-p}{n-p-s} \geq h(\hat{e}) \qquad (7)$$

where $R_C(\text{optimal})$ is adaptive coding rate R.

$$R = 1 - f(n, \varepsilon, \hat{e})h(\hat{e}) \qquad (8)$$

$$s = ((k/n) - R(1-\delta))n \qquad (9)$$

$$p = d - s \qquad (10)$$

Step 4) *Decoding*: *Bob* received syndromes S^X, and decodes his sequences Y_n which are constructed from the corresponding sequence p and s symbols in (9-10). This scheme is successfully concluded when *Bob* can produce his new syndrome $S^{X'}$ that matches the syndrome received from *Alice* $S^{X'} = S^X$ where $\Pr(X' = X)$ is equal to one. Otherwise, the feedback of decoding failure requests additional bits from the encoder by repeating to Step 2.

4. Numerical Results and Discussions

In the experimental setup, initial the all sifted keys are generated randomly according to error rates the entire range of QBER. The purpose reconciliation of the proposed method is to get no remaining error bit in the final reconciled keys with averaged values of 100 routines. The maximum number of iterations for LDPC decoding is 100. The mother codes of a parity check matrix **H** has a block length 200,000 bits [17].

Figure 2 shows the mean of estimated bit error rate $\hat{e}$ (estimated QBER) considered by a high code rate (modulated by $\delta = 0.1$) of four LDPC codes. The performance of the ML estimator is interpreted as that limitations for different mothor code's rates $R_C = 0.80$, $R_C = 0.70$, $R_C = 0.60$ and $R_C = 0.50$ are achieved approximately with QBER (1% – 11%). Therefore, this estimated method is suitable for rate-adaptive reconciliation scheme.

Next, reconciliation efficiency f which is used to measure the system performance, is defined (11) by the ratio of disclosed information during the reconciliation step ($leak_{recon}$) to the Slepian-Wolf bound $H(X|Y)$

$$f = \frac{leak_{recon}}{H(X|Y)} = \frac{1-R_C}{h(e)} = \frac{n-k-p}{(n-p-s)\cdot h(e)} \qquad (11)$$

Figure 3 presents that the proposed rate-adaptive LDPC codes with mother code's rates R_C are 0.8, 0.7, 0.6, and 0.5 modulated by $\delta = 0.1$ offers a better performance in terms of reconciliation efficiency than rate-fix LDPC codes and Cascade protocols as a function of QBER.

In Figure 4, the secret key throughput for BB84 QKD protocol is calculated as a function of distance using [18].

with the really inherent factors of the single photon source and detection. This ensures significantly for practical systems, when the reconciliation schemes are considered, particularly in the case of high-speed QKD devices. This secret key throughput simulation is computed from the performance of the real QKD devices, which enables operation at the clock rate of 1 GHz over $\alpha = 0.2$ dB/km losses in optical fiber, a dark counts probability of $\rho_d = 10^{-5}$, a detection efficiency of $\beta = 0.1$, and a protocol efficiency of $\xi = 0.5$. The secret key throughput performance of the proposed scheme is illustrated in Figure 4 in comparison with other existing schemes including the Cascade, rate-fix LDPC codes with estimated QBER by 10% of key sampling, and also with the theoretical limit on perfect reconciliation in the subject of distance.

5. Conclusions

This paper has proposed the efficient rate-adaptive LDPC reconciliation based Slepian-Wolf coding method by estimated QBER and reconciliation efficiency for quantum key distribution. The results show that rate-adaptive LDPC reconciliation has good performances in terms of reconciliation efficiency as function of QBER and secret key throughput with achieving the longest distances. Furthermore, this method can reduce the interactive communications between *Alice* and *Bob.* Therefore, it is suitable to high-speed QKD application.

Acknowledgement

This work was partially supported by Institute of Research and Development, Phranakhon Rajabhat University, Grant 26.01/2558 and Thailand Graduate Institute of Science and Technology (TGIST), National Science and Technology Development Agency (NSTDA), No. TG-44-09-55-039M.

The authors would like to thank all researchers of Optical and Quantum Communications Laboratory (OQC), NECTEC, NSTDA for their helpful suggections.

References

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing,* Bangalore, India (IEEE, New York, 1984), pp. 175–179, 1984

[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin. "Experimental quantum cryptography," J. *Cryptol,* 5:3–28, 1992.

[3] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," *Advance in Cryptology Proc. EUROCRYPT 93*, pp. 410–423, 1994.

[4] W. T. Buttler, S. K. Lamoreaux, J.R. Torgerson, G.H. Nickel, C.H. Donahue and C.G. Peterson, "Fast, Efficient Error Reconciliation for Quantum Cryptography," *Physical Review A (Atomic, Molecular and Optical Physics)*, vol. 67, 052303, 2003.

[5] P. Treeviriyanupab, P. Sangwongngam, K. Sripimanwat, O. Sangaroon, "BCH-Based Slepian-Wolf Coding with Feedback Syndrome Decoding for Quantum Key Reconciliation", *ECTI-CON 2012*, Hua Hin, Thailand, pp.1-4, May16 – 18, 2012.

[6] D. Elkouss, A. Leverrier, R. Alléaume, and J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," *in Proc. 2009 IEEE International Symposium on Information Theory*, pp. 1879–1883, Jul. 2009.

[7] D. Elkouss, J. Martinez, D. Lancho, and V. Martin, "Rate Compatible Protocol for Information Reconciliation: An application to QKD," *in IEEE Information Theory Workshop,* pp. 145–149, Jan. 2010.

[8] T. Phromsa-ard, P. Sangwongngam, K. Sripimanwat, K. Kaemarungsri, P. Vanichchanunt, and L. Wuttisittikulkij. "Low-complexity key reconciliation algorithm using ldpc bit-flipping decoding for quantum key distribution." *ECTI-CON 2014*, pp 1–5, May 2014.

[9] P. Treeviriyanupab, T. Phromsa-ard, C. Zhang, M. Li, P. Sangwongngam, T. Sanevong Na Ayutaya, N. Songneam, R. Rattanatamma, C. Ingkavet, W. Sanor, W. Chen, Z. Han, and K. Sripimanwat,"Rate-adaptive reconciliation and its estimator for quantum bit error rate," *ISCIT2014*, pp 351-355, Incheon, Korea, 2014.

[10] D. MacKay and R. Neal, "Near Shannon limit performance of low density parity check codes*," IEEE Electronics Letters*, vol. 32, no.18, pp. 1645-1655, 29th Aug. 1996.

[11] D. MacKay, "Good error correcting codes based on very sparse matrices," IEEE Trans. *Information Theory*, pp. 399-431, March 1999.

[12] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[13] A. Liveris, Z. Xiong, and C. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes*," IEEE Communications Letters*., vol. 6, no. 10, pp. 440–442, Oct. 2002

[14] V. Toto-Zarasoa, A. Roumy, C. Guillemot, "Maximum likelihood BSC parameter estimation for the Slepian-Wolf problem," *IEEE Communications Letters*, pp 232–234, vol 15, 2011.

[15] G. Lechner and C. Pacher, "Estimating channel parameters from the syndrome of a linear code, *IEEE Communications Letters*, Vol. 17, Issue 11, pp 2148 – 2151, 2013.

[16] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, "Fundamental finite key limits for information reconciliation in quantum key distribution," *in 2014 IEEE International Symposium on Information Theory (ISIT)*, pp. 1469-1473, 2014

[17] A list of low-density parity-check codes and matrices. *Available*: http://gcc.ls.fi.upm.es/en/codes.html

[18] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *in. Proceedings. International Symposium on Information Theory, ISIT 2004* , p. 136, 2004.